Start AM 7.0.0 with external DS over a secure connection

As of the release of AM 7.0.0 and DS 7.0.0 LDAP connections to DS are now secure by default. This means the port number has changed from the default of `1389` to `1636` and the SSL/TLS feature should now be used. It is not possible to use DS without these changes from DS 7.0.0 onwards.

Engineers looking to setup AM with an external DS will need to follow a new process. This guide covers the process of setting up a truststore and installing AM with an external DS configuration store for both DS version 7 and older versions of DS.

Step-by-step guide

The following steps take you through the process of setting up the AM truststore with the DS self-signed certificate in it.

Create AM truststore

Create a truststore by copying the JDK provided truststore. The following commands give us an example of how to do this:

```
$ mkdir -p $HOME/openam/security/keystores
$ cp $JAVA_HOME/lib/security/cacerts $HOME/openam/security/keystores/truststore
```

Optional: If required the password of the truststore can be changed from the default "changeit" to another password. The following command shows how to do this:

```
$ keytool -storepasswd -keystore $HOME/openam/security/keystores/truststore

Enter keystore password: changeit
New keystore password: badger
Re-enter new keystore password: badger
```

If you do choose to change this password, be sure to update the "`javax.net.ssl.trustStorePassword`" value in subsequent commands.

Start DS 7.0.0

With the truststore created we can now setup DS. For DS 7.0.0 there have been some changes to the `setup` command. Of note is the inclusion of the `--deploymentKey` and `--deploymentKeyPassword` options.

- Download DS

The following steps show setting up the server with the following fixed credentials:

- Deployment Key of "AForYBg8mR_0kRsWbGHSrUP8aApOtpw5CBVN1bkVDAKLAd0oCRgow6hc"
- Deployment Key Password of "`password`"

This will create a server we can use for testing.

```
$ echo "administrator" > /tmp/admin.pwd
$ ./setup \
    --deploymentKey AForYBg8mR_0kRsWbGHSrUP8aApOtpw5CBVN1bkVDAKLAd0oCRgow6hc \
    --deploymentKeyPassword password \
    --rootUserDN "cn=Directory Manager" \
    --rootUserPasswordFile /tmp/admin.pwd \
    --monitorUserPasswordFile /tmp/admin.pwd \
    --hostname ds.localtest.me \
    --ldapPort 1389 \
    --ldapsPort 1636 \
    --httpsPort 8443 \
    --adminConnectorPort 4444 \
    --profile am-config \
    --set am-config/baseDn:ou=am-config \
    --set am-config/amConfigAdminPassword:administrator \
    --profile am-identity-store \
    --set am-identity-store/amIdentityStoreAdminPassword:administrator \
    --profile am-cts \
    --set am-cts/amCtsAdminPassword:administrator \
    --acceptLicense
```

The installation will then proceed with the following output:

```
Validating parameters..... Done
Configuring certificates......... Done

Store the following deployment key in a safe place and re-use it when
configuring other servers in the topology:

AForYBg8mR_0kRsWbGHSrUP8aApOtpw5CBVN1bkVDAKLAd0oCRgow6hc

Configuring server..... Done
Configuring profile AM configuration data store......... Done
Configuring profile AM identity data store......... Done
Configuring profile AM CTS data store.............. Done

To see basic server status and configuration, you can launch
/opt/opendj/bin/status
```

The Deployment Key is either provided or output in the setup log. If it is not provided it will be generated on each installation.

For older methods of installing DS, check the appropriate getting started guide.

Copy ca-cert from the generated keystore into the AM trust store

There are two approaches for how to do this. One for DS 7+ only, and relies on the knowledge of the `deploymentKey` and the `deploymentKeyPassword`, and uses the DS-provided `dskeymgr` tool; and one that does not rely on knowledge of these two parameters, and can be executed with older versions of DS.

DS without deploymentKey, including older DS versions

Read the password for the locally installed DJ from the generated **keystore.pin** file in the installed DJ config directory:

```
$ more /path/to/opendj/config/keystore.pin
pfOcIDBdDWfVcjWGXMMNRqixH/bMKXC/hdVA+ZMBkuvkEHhWY5e9Gl7O+s16rlaW1tE=
```

Copy the ca-cert certificate from the keystore into the AM truststore:

```
$ keytool -importkeystore -srckeystore /path/to/opendj/config/keystore -srcstorepass pfOcIDBdDWfVcjWGXMMNRqixH
/bMKXC/hdVA+ZMBkuvkEHhWY5e9Gl7O+s16rlaW1tE= -destkeystore /path/to/openam/openam-truststore.jks -deststorepass
changeit -srcalias ca-cert
```

DS 7 (with deploymentKey)

Execute the following command from within the DS folder to export the self-signed certificate and store it into a file in the AM installation folder.

Note: We need both the Deployment Key and the Deployment Key Password to access the keystore.

```
$ bin/dskeymgr export-ca-cert \
  --deploymentKey AForYBg8mR_0kRsWbGHSrUP8aApOtpw5CBVN1bkVDAKLAd0oCRgow6hc \
  --deploymentKeyPassword password > $HOME/openam/ds-ca-cert.pem
```

Inspect the contents of this certificate to verify it is an X.509 certificate:

```
$ cat $HOME/openam/ds-ca-cert.pem
-----BEGIN CERTIFICATE-----
MIIBfzCCASSgAwIBAgILAPyH9tZsACMAsAQwCgYIKoZIzj0EAwIwMTEWMBQGA1UE
ChMNRm9yZ2VSb2NrLmNvbTEXMBUGA1UEAxMORGVwbG95bWVudCBrZXkwHhcNMjAw
ODA3MDg0MjU0WhcNMzAwODA1MDg0MjU0WjAxMRYwFAYDVQQKEw1Gb3JnZVJvY2su
Y29tMRcwFQYDVQQDEw5EZXBsb3ltZW50IGtleTBZMBMGByqGSM49AgEGCCqGSM49
AwEHA0IABLYyEy3IKgGpO7RpSTh9EyVHfGfhOV9i0CQtYUfP2KIBHgPFOmpxVKIh
lgugW93FqnWt0siq6LgH02XcZTRWFPajIzAhMA4GA1UdDwEB/wQEAwIBBjAPBgNV
HRMBAf8EBTADAQH/MAoGCCqGSM49BAMCA0kAMEYCIQC/8wnMqwzPKyaTvGKB1eFq
/DueScqOsk0CJY0ASWyS8QIhAOCpTjtelgZdGq1DOStKJW6vAEWo4oG1cuZ5zWmX
qpPe
-----END CERTIFICATE-----
```

Import the DS self-signed certificate into the AM truststore with the following command:

```
$ keytool -importcert -file $HOME/openam/ds-ca-cert.pem \
    -keystore $HOME/openam/security/keystores/truststore \
    -storepass changeit -alias ds-ca-cert -noprompt
Certificate was added to keystore
```

Start DS

At this point we can now start DS with the following command:

```
$ bin/start-ds
```

We can then verify the status of the started server with the following:

```
$ bin/status -h ds.localtest.me -p 1636 -D "cn=Directory Manager" -w administrator --useJavaTrustStore $HOME/openam
/security/keystores/truststore
```

Define `javax.net.ssl` System Properties

Finally, before we can start AM we need to define the Java truststore override options to tell AM where the truststore is. This will allow AM to connect to the DS server:

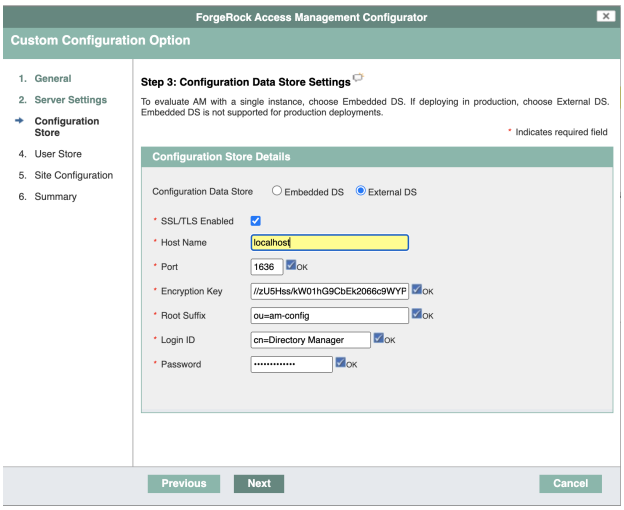
```
$ export JAVA_OPTS="-Djavax.net.ssl.trustStore=$HOME/openam/security/keystores/truststore \
    -Djavax.net.ssl.trustStorePassword=changeit \
    -Djavax.net.ssl.trustStoreType=jks"
```

Then proceed to start AM and step through the configuration process.

AM Configuration

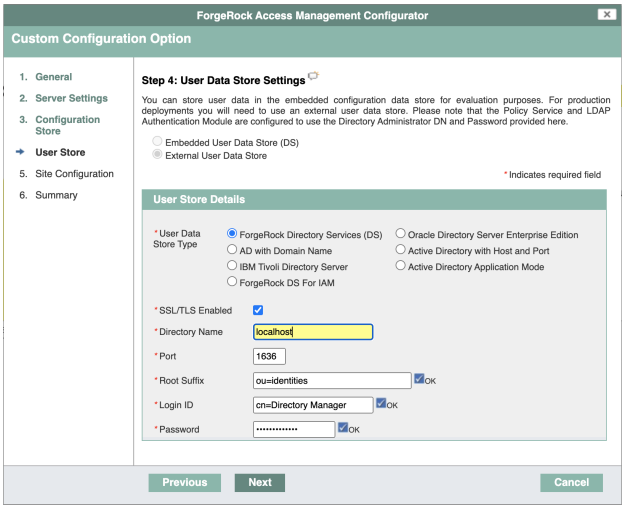
If we are using the DS server configured in the above guide then the following are the configuration screens for the Configuration Data Store and User Store pages.

Configuration Data Store



- SSL/TLS Enabled: True
- Hostname: localhost
- Port: 1636
- Root Suffix: ou=am-config
- Login ID: cn=Directory Manager
- Password: administrator

User Store



- SSL/TLS Enabled: True
- Directory Name: localhost
- Port: 1636
- Root Suffix: ou=identities
- Login ID: cn=Directory Manager
- Password: administrator

Related articles

- Start AM 7.0.0 with external DS over a secure connection